UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/659,368	09/11/2003	Brian N. Belanger	2222.3810000	3018

26111 7590 10/07/2011

STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C.
1100 NEW YORK AVENUE, N.W.
WASHINGTON, DC 20005

EXAMINER	
JOHNSON, CARLTON	

ART UNIT	PAPER NUMBER
2436	

MAIL DATE	DELIVERY MODE
10/07/2011	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/659,368	BELANGER ET AL.	
	Examiner	Art Unit	
	CARLTON JOHNSON	2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11 July 2011*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

5)☒ Claim(s) *1-38 and 41-44* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1-38 and 41-44* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

12)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. In view of the Appeal Brief filed on 7/11/2011, PROSECUTION IS HEREBY REOPENED. A new ground of rejection is set forth below.

To avoid abandonment of the application, appellant must exercise one of the following two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37 CFR 1.113 (if this Office action is final); or,

(2) request reinstatement of the appeal.

If reinstatement of the appeal is requested, such request must be accompanied by a supplemental appeal brief, but no new amendments, affidavits (37 CFR 1.130, 1.131 or 1.132) or other evidence are permitted. See 37 CFR 1.193(b)(2).

A Supervisory Patent Examiner (SPE) has approved of reopening prosecution by signing below:

/Nasser Moazzami/

Supervisory Patent Examiner, Art Unit 2436.

2. Claims **1 - 38, 41 - 44** are pending. Claims **39, 40** have been cancelled. Claims **1, 7, 15, 16, 23, 24, 29, 30** are independent. This application was filed on 9-11-2003.

Response to Arguments

3. Applicant's arguments have been fully considered but they were partially persuasive. Therefore, new grounds of rejection have been entered.

A. Applicant argues on pages 21-27 of Remarks *that Claims 1, 7, 16, 24, 29, and 30 are the independent claims. Independent claim 1 recites at least the following distinguishing feature: "wherein the access candidate attributes are revisable based, at least in part, on a determination indicating that access to the first level is prohibited." Independent claims 7, 16, 24, 29, and 30 recite similar distinguishing features, using analogous language.*

The Examiner disagrees. Timson, Moreh, and Bacha are no longer used as grounds of rejection. The arguments directed towards Timson, Moreh, and Bacha are moot. Lee is used to disclose a low level authentication process which is analogous to a first security level (see Lee col 3, ll 26-30: transactions presented for authorization (analogous to request for access); col 7, lines 12-16: information passed to access device; access device using access device applications (computational resources, software) performs low level (first level) authentication) and a high level authentication process which is analogous to a second security level. (see Lee col 8, ll 44-50: high level (second level) authentication, steps to verify that card is valid and validly issued; col 8, ll 60-64: upon completion of high level (second level) authentication, transaction counter is incremented; (determination that high level authentication is successful))

In addition, Lee discloses that authentication results are revisable such that when an authentication result is unsuccessful, then the resolution result can be forward to an authorization system for a resolution. (see Lee col 9, lines 21-27: passes low level authentication and does not pass high level authentication (or vice versa); col 9, lines

21-27: if high level (second level) did not pass (not successful); information passed to authorization system for resolution; (authentication result can be revised based on resolution action))

And, Te specifically discloses the capability to access a resolution entity in the event that an access authentication attempt for a level of authentication is unsuccessful. (see Te col 6, lines 50-59: conflict presented by specific access mode resolved by resolution mode; col 7, lines 3-4: access conflict is resolved via the resolution mode)

B. Applicant argues on page 27 of Remarks *that at least based on their respective dependencies to claims 1, 7, 16, 24, and 30, claims 2-4, 8-10, 14, 17-19, 25, 26, 31-33, 37, and 38 should be found allowable over the applied references.*

The Examiner disagrees since arguments against the dependent claims are also answered by responses to the arguments against the independent claims.

C. Applicant argues on page 29 of Remarks *independent Claims 15 and 23*

The Examiner disagrees since independent claims 15 and 23 have similar limitations as independent claim 1. Responses to arguments for independent claim 1 answer arguments against independent claims 15 and 23. In addition, Orsini is not used to disclose the indicated claim limitation. The Office Action indicates the claim limitation Orsini is used to reject.

D. Applicant argues on page 30 of Remarks *that claims 1, 7, 15, 16, 24, and 30, claims 5, 6, 11-13, 20.22, 27, 28, 34-36, and 41-44 should be found allowable over the applied references.*

The Examiner disagrees since arguments against the dependent claims are also answered by responses to the arguments against the independent claims.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

5. Claims **1, 7, 15, 16, 24, 29, 30** are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. There does not appear to be disclosure for the following claim limitation: *"wherein the access candidate attributes are revisable based, at least in part, on a determination indicating that access to the first level is prohibited"*. The Examiner will interpret this claim limitation as the capability to modify the authentication results from the first level or the second level with a resolution entity.

Appropriate correction is required.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims **1 - 4, 7 - 10, 14, 16 - 19, 24 - 26, 29 - 33, 37, 38** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Lee et al.** (US Patent No. **6,003,014**) in view of **Te et al.** (US Patent No. **6,978,381**).

Regarding Claims 1, 7, 24, 29, Lee discloses a method comprising:

a) receiving, using a processing device, a first request, from a first sponsor of an access candidate, for access to a first security level in a computer network, wherein the first security level secures computational resources for accessing electronic data (see Lee col 3, ll 26-30: transactions presented for authorization (analogous to request for access); col 7, lines 12-16: information passed to access device; access device using access device applications (computational resources and software) performs low level (first level) authentication)

Furthermore, Lee discloses the following:

b) determining, using the processing device, whether access candidate attributes satisfy access requirements of the resources, wherein the access candidate

attributes are revisable based, at least in part, on a determination indicating that access to the first level is prohibited, (see Lee col 9, lines 21-27: passes low level authentication and does not pass high level authentication (or vice versa); col 9, lines 21-27: if high level (second level) did not pass (not successful); information passed to authorization system for resolution; (authentication result can be revised based on resolution action))

c) granting, using the processing device, access to the first security level based on a determination indicating that access to the first level is not prohibited; (see Lee col 3, ll 32-36: perform a first or low-level authentication ; if authentication is successful, access is granted)

d) receiving, using the processing device, a second request, from a second sponsor of the access candidate, for access to a second security level in the computer network in response to the granting of access to the first security level, wherein the second security level secures the electronic data; (see Lee col 8, ll 44-50: high level (second level) authentication, steps to verify that card is valid and validly issued)

e) determining, using the processing device, whether attributes of the access candidate satisfy access requirements of the electronic data secured by the second security level; (see Lee col 8, ll 60-64: upon completion of high level (second level) authentication, transaction counter is incremented; (determination that high level authentication is successful))

Lee discloses for f): obtaining authorization for the second request if the access

candidate attributes fail to satisfy the access requirement of the electronic data in response to a determination indicating that access to the second security level is prohibited; (see Lee col 9, ll 21-27: instances where access device passes low level (first level) authentication and does not pass high level (second level) authentication; information passed to authorization system for resolution)

Lee does not specifically disclose obtaining authorization from a resolution authority and granting the access candidate access.

However, Te discloses for f): obtaining authorization for request from a resolution authority; and for g): in response to obtaining the authorization from the resolution authority (see Te col 6, lines 50-59: conflict presented by specific access mode resolved by resolution mode) granting the access candidate access to the second security level. (see Te col 7, lines 3-4: access conflict is resolved via the resolution mode)

It would have been obvious to one of ordinary skill in the art to modify Lee for obtaining authorization from a resolution authority and granting the access candidate access as taught by Te. One of ordinary skill in the art would have been motivated to employ the teachings of Te for the benefits achieved from enhancements to controls thereby providing a reduction in user burden obtaining access to resources and administration burden in implementing and updating access authorizations. (see Te col. 1, lines 10-15)

Regarding Claims 2, 8, 17, 25, 31, Lee discloses the method of Claims 1, 8, 16, 24,

30, further comprising granting access to the second security level in response to a determination indicating that access by the access candidate is not prohibited. (see Lee col 8, lines 60-64: upon completion of high level authentication (second security level) transaction counter is incremented)

Regarding Claims 3, 9, 18, 32, Lee discloses the method of Claims 1, 7, 16, 30, further comprising denying access to the second security level if denied the third request. (see Lee col 9, lines 21-27: passes low level authentication (first security level) and does not pass high level authentication (second security level)

Lee does not specifically disclose a resolution authority.

However, Te discloses a resolution authority. (see Te col 6, lines 50-59: any conflict to specific access mode resolved by a resolution mode)

It would have been obvious to one of ordinary skill in the art to modify Lee for a resolution authority as taught by Te. One of ordinary skill in the art would have been motivated to employ the teachings of Te for the benefits achieved from enhancements to controls thereby providing a reduction in user burden obtaining access to resources and administration burden in implementing and updating access authorizations. (see Te col. 1, lines 10-15)

Regarding Claims 4, 10, 19, 26, 33, Lee discloses the method of Claims 1, 7, 16, 24, 30.

Lee does not specifically disclose a graphical display associated with the access

candidate and accessed for display.

However, Te discloses wherein at least one of the access requirements of the resources and the access requirements of the electronic data are represented as part of a graphical display associated with the access candidate and accessed for display to a controller via a network. (see Te col 15, lines 9-14: assets to be added to profile can be retrieved from asset list and displayed as a menu; (menu denotes a graphical display))

It would have been obvious to one of ordinary skill in the art to modify Lee for a graphical display associated with the access candidate and accessed for display as taught by Te. One of ordinary skill in the art would have been motivated to employ the teachings of Te for the benefits achieved from enhancements to controls thereby providing a reduction in user burden obtaining access to resources and administration burden in implementing and updating access authorizations. (see Te col. 1, lines 10-15)

Regarding Claims 14, 37, Lee discloses the method of Claims 7, 30, wherein at least one of the request for physical access or the request for access to the electronic data is submitted by more than one sponsor of the access candidate. (see Lee col 5, lines 40-44: staging computer communicates with any number of terminals (access candidates) to collect batches of transactions)

Regarding Claim 16, Lee discloses a system for providing an access candidate access to secured electronic data, the system comprising:

a) storage means for receiving and storing electronic data using a computer network; (see Lee col 2, lines 52-54: making transactions over open network such as the Internet (network communications); col 9, lines 21-27: terminal stores authorized and failed transaction information data store)

Furthermore, Lee discloses the following:

b) means for evaluating a first request for access to the one or more resources, in the computer network, wherein the resources secure the electronic data, and wherein an evaluation of the first request includes a first comparison of one or more attributes of the access candidate with one or more access requirements associated with the resources, and wherein the one or more attributes of the access candidate are revisable if the first comparison indicates that access is prohibited; (see Lee col 9, lines 21-27: passes low level authentication and does not pass high level authentication (or vice versa); col 9, lines 21-27: if high level (second level) did not pass (not successful); information passed to authorization system for resolution; (authentication result can be revised based on resolution action))

c) means for granting access to the one or more resources if the first comparison indicates that access is not prohibited; (see Lee col 7, lines 27-30: if low level (first level) authentication produces satisfactory result, access device authorizes access)

d) means for evaluating a second request for access to the electronic data by the one or more resources, wherein an evaluation of the second request includes a

second comparison of one or more attributes of the access candidate with one or more access requirements associated with the electronic data; (see Lee col 8, ll 44-50: high level (second level) authentication, steps to verify that card is valid and validly issued)

e) means for obtaining authorization for the second request, if the one or more attributes of the access candidate fails to satisfy one or more access requirements associated with the electronic data in response to the evaluation of the second request indicating that access to the electronic data is prohibited; (see Lee col 9, lines 21-27: passes low level authentication and does not pass high level authentication (or vice versa); col 9, lines 21-27: if high level (second level) did not pass (not successful); information passed to authorization system for resolution; (authentication result can be revised based on resolution action))

f) means for granting access to the electronic data using the one or more resources in response to obtaining the authorization. (see Lee col 8, ll 60-64: upon completion of high level (second level) authentication, transaction counter is incremented; (determination that high level authentication is successful))

Lee does not specifically disclose obtaining authorization from a resolution authority. However, Te discloses obtaining the authorization from the resolution authority. (see Te col 6, lines 50-59: any conflict to specific access mode resolved by a resolution mode; col 7, lines 3-4: access conflict is resolved via the resolution mode)

It would have been obvious to one of ordinary skill in the art to modify Lee for obtaining authorization from a resolution authority as taught by Te. One of ordinary

skill in the art would have been motivated to employ the teachings of Te for the benefits achieved from enhancements to controls thereby providing a reduction in user burden obtaining access to resources and administration burden in implementing and updating access authorizations. (see Te col. 1, lines 10-15)

Regarding Claim 30, Lee discloses an article of manufacture including a non-transitory computer-readable medium having instructions stored thereon, execution of which causes a processing device to perform operations comprising:

a) receiving, using a processing device, a request for access to a first security level in a computer network; (see Lee col 3, ll 26-30: transactions presented for authorization (analogous to request for access); col 7, lines 12-16: information passed to access device; access device using access device applications (computational resources, software) performs low level (first level) authentication)

Furthermore, Lee discloses the following:

b) comparing, using a processor device, one or more attributes of an access candidate with one or more access requirements associated with the first security level, wherein the one or more attributes of the access candidate are revisable based, at least in part, on a determination indicating that access by the access candidate to the first security level is prohibited; (see Lee col 9, lines 21-27: passes low level authentication and does not pass high level authentication (or vice versa); col 9, lines 21-27: if high level (second level) did not pass (not successful); information passed to authorization system for resolution;

(authentication result can be revised based on resolution action))

c) granting, using the processing device, access to the first security level based on a comparison indicating that access by the access candidate to the first security level is not prohibited; (see Lee col 3, ll 32-36: perform a first or low-level authentication ; if authentication is successful, access is granted)

d) receiving, using the processing device, a request for access to a second security level in the computer network; (see Lee col 8, ll 44-50: high level (second level) authentication, steps to verify that card is valid and validly issued)

Lee does not specifically disclose obtaining authorization from a resolution authority. However, Te discloses:

e) obtaining authorization for the request in response to a comparison indicating that access by the access candidate is prohibited. (see Te col 6, lines 50-59: any conflict to specific access mode resolved by a resolution mode; col 7, lines 3-4: access conflict is resolved via the resolution mode)

It would have been obvious to one of ordinary skill in the art to modify Lee for obtaining authorization from a resolution authority as taught by Te. One of ordinary skill in the art would have been motivated to employ the teachings of Te for the benefits achieved from enhancements to controls thereby providing a reduction in user burden obtaining access to resources and administration burden in implementing and updating access authorizations. (see Te col. 1, lines 10-15)

Regarding Claim 38, Lee discloses the method as in claim 1, further comprising

determining the authorization by granting a waiver of the access requirements. (see Lee col 9, lines 21-27: information is passed to authorization system for resolution; implies authentication results are changeable by resolution entity))

8. Claims **5, 6, 11 - 13, 15, 20 - 23, 27, 28, 34 - 36, 41 - 44** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Lee** in view of **Te** and further in view of **Orsini et al.** (US PGPUB No. **20040049687**).

Regarding Claims 5, 11, 13, 27, Lee discloses the method of Claims 1, 7, 24, wherein the access requirements. (see Lee col 12, lines 31-38: information used to prove the fact of the transaction (successful processing of the transaction); access device identifying information)

Lee does not specifically disclose the access requirements comprise a citizenship status of the access candidate or a current location of the access candidate.

However, Orsini discloses wherein at least one of access requirements of the resource and the access requirements of the electronic data comprise a citizenship status of the access candidate or a current location of the access candidate. (see Orsini paragraph [0013], lines 1-3; paragraph [0060], lines 4-13: management of secure data, parameters (i.e. attributes) agreement, location information)

It would have been obvious to one of ordinary skill in the art to modify Lee for one or more access requirements related to at least one of a citizenship status of the access candidate and a current location of the access candidate as taught by Orsini. One of

ordinary skill in the art would have been motivated to employ the teachings of Orsini for a relatively fast, secure, and efficient authentication of data streams. (see Orsini paragraph [0012], lines 1-3; paragraph [0013], lines 1-3)

Regarding Claims 6, 12, 22, 28, 36, Lee discloses the method of Claims 5, 11, 16, 27, 30, wherein the one or more attributes of the access candidate. (see Lee col 12, lines 31-38: information used to prove the fact of the transaction (successful processing of the transaction); access device identifying information)

Lee does not specifically disclose attributes comprise a citizenship status of the access candidate or a current location of the access candidate.

However, Orsini discloses wherein one or more attributes of the access candidate relate to the at least one of a citizenship status of the access candidate or a current location of the access candidate. (see Orsini paragraph [0013], lines 1-3; paragraph [0060], lines 4-13: management of secure data, parameters (i.e. attributes) agreement, location information)

It would have been obvious to one of ordinary skill in the art to modify Lee for attributes comprise a citizenship status of the access candidate or a current location of the access candidate as taught by Orsini. One of ordinary skill in the art would have been motivated to employ the teachings of Orsini for a relatively fast, secure, and efficient authentication of data streams. (see Orsini paragraph [0012], lines 1-3; paragraph [0013], lines 1-3)

Regarding Claim 15, Lee discloses a method comprising:

a) identifying, using a processing device, a plurality of data subsets of the electronic data, wherein respective data subsets correspond to respective sets of access requirements; (see Lee col 5, lines 40-44: staging computer communicates with any number of terminals (access candidates) to collect batches of transactions; col 12, lines 31-38: information used to prove the fact of the transaction (successful processing of the transaction); access device identifying information)

Furthermore, Lee discloses the following:

d) determining, using the processing device, whether the access candidate attributes satisfy access requirements of the first security level, wherein the access candidate attributes are revisable based, at least in part, on a determination indicating that access to the first security level is prohibited; (see Lee col 9, lines 21-27: passes low level authentication and does not pass high level authentication (or vice versa); col 9, lines 21-27: if high level (second level) did not pass (not successful); information passed to authorization system for resolution; (authentication result can be revised based on resolution action))

e) granting, using the processing device, access to the first security level based on a determination indicating that access to the first security level is not prohibited; (see Lee col 7, lines 27-30: if low level (first level) authentication produces satisfactory result, access device authorizes access)

g) determining, using the processing device, whether attributes of the access candidate satisfy the respective set of access requirements corresponding to the

at least one of the plurality of data subsets; (see Lee col 8, ll 60-64: upon completion of high level (second level) authentication, transaction counter is incremented; (determination that high level authentication is successful))

i) in response to obtaining the authorization granting access to the second security level. (see Lee col 8, ll 60-64: upon completion of high level (second level) authentication, transaction counter is incremented; (determination that high level authentication is successful))

Furthermore, Lee discloses

for b): determining, using the processing device, at least one data class associated with the respective data subsets (see Lee col 3, ll 26-30: transactions presented for authorization (analogous to request for access); col 7, lines 12-16: information passed to access device; access device using access device applications (computational resources, software) performs low level (first level) authentication), and

for c): receiving, using the processing device, a first request, from a first sponsor of the access candidate, for access to a first security level in a computer network, wherein the first security level secures physical access to a computer workstation for accessing the electronic data, (see Lee col 3, ll 26-30: transactions presented for authorization (analogous to request for access); col 7, lines 12-16: information passed to access device; access device using access device applications (computational resources, software) performs low level (first level) authentication) and

for f): receiving, using the processing device, a second request, a second sponsor of the access candidate, for access to a second security level in the computer network in response to the granting of access to the first security level, wherein the second security level secures access to at least one of the plurality of data subsets; (see Lee col 8, ll 44-50: high level (second level) authentication, steps to verify that card is valid and validly issued)

Furthermore, Lee discloses for h): obtaining authorization for the second request if the access candidate attributes fail to satisfy the respective set of access requirements corresponding to the at least one of the plurality of data subsets in response to a determination indicating that access to the at least one of the plurality of data subsets is prohibited. (see Lee col 9, lines 21-27: passes low level authentication and does not pass high level authentication (or vice versa); col 9, lines 21-27: if high level (second level) did not pass (not successful); information passed to authorization system for resolution; (authentication result can be revised based on resolution action))

Lee does not specifically disclose obtaining authorization from a resolution authority. However, Te discloses for h): obtaining authorization from a resolution authority. (see Te col 6, lines 50-59: any conflict to specific access mode resolved by a resolution mode; col 7, lines 3-4: access conflict is resolved via the resolution mode)

It would have been obvious to one of ordinary skill in the art to modify Lee to use authentication services such as a resolution authority as taught by Te. One of

ordinary skill in the art would have been motivated to employ the teachings of Te for the benefits achieved from enhancements to controls thereby providing a reduction in user burden obtaining access to resources and administration burden in implementing and updating access authorizations. (see Te col. 1, lines 10-15)

Lee-Te does not specifically disclose an indication of a citizenship status of the access candidate, an indication of a current location of the access candidate, and an indication of an existence of a data access agreement with the access candidate. However, Orsini discloses the following:

b) at least a citizenship requirement and a location requirement for access to data associated with the at lease one data class; (see Orsini paragraph [0013], lines 1-3; paragraph [0060], lines 4-13: management of secure data, parameters (i.e. attributes) agreement, location information)

c) an indication of a citizenship status of the access candidate, an indication of a current location of the access candidate, and an indication of an existence of a data access agreement with the access candidate; (see Orsini paragraph [0013], lines 1-3; paragraph [0060], lines 4-13: management of secure data, parameters (i.e. attributes) agreement, location information, citizenship information)

It would have been obvious to one of ordinary skill in the art to modify Lee-Te for the request including an indication of a citizenship status of the access candidate, an indication of a current location of the access candidate, and an indication of an existence of a data access agreement with the access candidate as taught by Orsini. One of ordinary skill in the art would have been motivated to employ the teachings of

Orsini for a relatively fast, secure, and efficient authentication of data streams. (see Orsini paragraph [0012], lines 1-3; paragraph [0013], lines 1-3)

Regarding Claim 20, Lee discloses the system of Claim 16, wherein one or more access requirements. (see Lee col 12, lines 31-38: information used to prove the fact of the transaction (successful processing of the transaction); such as access device identifying information)

Lee does not specifically disclose at least one of: a valid data access agreement with a potential access candidate; a current location of the potential access candidate; and a citizenship status of the potential access candidate.

However, Orsini discloses wherein at least one of the one or more access requirements associated with the resources and the one or more access requirements associated with the electronic data relates to at least one of: a valid data access agreement with a potential access candidate; a current location of the potential access candidate; and a citizenship status of the potential access candidate. (see Orsini paragraph [0013], lines 1-3; paragraph [0060], lines 4-13: management of secure data, parameters (i.e. attributes) agreement, location information)

It would have been obvious to one of ordinary skill in the art to modify Lee for at least one of: a valid data access agreement with a potential access candidate; a current location of the potential access candidate; and a citizenship status of the potential access candidate as taught by Orsini. One of ordinary skill in the art would have been motivated to employ the teachings of Orsini for a relatively fast, secure, and efficient

authentication of data streams. (see Orsini paragraph [0012], lines 1-3; paragraph [0013], lines 1-3)

Regarding Claims 21, 34, 35, Lee discloses the system of Claims 20, 30, 34, wherein attributes of the access candidate. (see Lee col 12, lines 31-38: information used to prove the fact of the transaction (successful processing of the transaction); such as access device identifying information)

Lee does not specifically disclose at least one of: an indication of an existence of a data access agreement with the access candidate; a current location of the access candidate; and a citizenship status of the access candidate.

However, Orsini discloses wherein at least one of: an indication an existence of a data access agreement with the access candidate; a current location of the access candidate; or a citizenship status of the access candidate. (see Orsini paragraph [0013], lines 1-3; paragraph [0060], lines 4-13: management of secure data, parameters (i.e. attributes) agreement, location information)

It would have been obvious to one of ordinary skill in the art to modify Lee for at least one of: an indication an existence of a data access agreement with the access candidate; a current location of the access candidate; and a citizenship status of the access candidate as taught by Orsini. One of ordinary skill in the art would have been motivated to employ the teachings of Orsini for a relatively fast, secure, and efficient authentication of data streams. (see Orsini paragraph [0012], lines 1-3; paragraph [0013], lines 1-3)

Regarding Claim 23, Lee discloses a system comprising:

a) storage configured to receive and store the electronic data using a computer network; (see Lee col 2, lines 52-54: making transactions over open network such as the Internet (network communications); col 9, lines 21-27: terminal stores authorized and failed transaction information data store)

Furthermore, Lee discloses the following:

b) one or more resources configured to process and manipulate the electronic data using a computer network; (see Lee col 2, lines 52-54: making transactions over open network such as the Internet (network communications); col 9, lines 21-27: terminal stores authorized and failed transaction information data store)

e) adapted to authorize access to one or more portions of the electronic data in response to a comparison performed by a corresponding data access controller indicates access is prohibited; (see Lee col 3, ll 32-36: perform a first or low-level authentication ; if authentication is successful, access is granted) and

f) a data access module configured to: evaluate a request for access to one or more portions of the electronic data by the one or more resources to identify one or more data access controllers corresponding to the one or more portions of the electronic data; (see Lee col 8, ll 60-64: upon completion of high level (second level) authentication, transaction counter is incremented; (determination that high level authentication is successful)) and

g) forward the request for access to the one or more identified data access

controllers for evaluation as to whether to grant the access candidate access to the corresponding one or more portions of the electronic data. (see Lee col 5, lines 6-9: terminal interface application forwards transaction information from access device)

Furthermore, Lee discloses wherein one or more data access controllers configured to grant access to a corresponding portion of the electronic data based at least in part on a comparison, and associated with one or more resources or data classes of the corresponding portion of the electronic data. (see Lee col 3, ll 32-36: perform a first or low-level authentication; if authentication is successful, access is granted)

Lee does not specifically disclose a resolution authority.
However, Te discloses a resolution authority. (see Te col 6, lines 50-59: any conflict to specific access mode resolved by a resolution mode; col 7, lines 3-4: access conflict is resolved via the resolution mode)

It would have been obvious to one of ordinary skill in the art to modify Lee for a resolution authority as taught by Te. One of ordinary skill in the art would have been motivated to employ the teachings of Te for the benefits achieved from enhancements to controls thereby providing a reduction in user burden obtaining access to resources and administration burden in implementing and updating access authorizations. (see Te col. 1, lines 10-15)

Lee-Te does not specifically disclose a citizenship status, a current location of the access candidate and an existence of a data access agreement with a citizenship

requirement, location requirement and data access agreement requirement. However, Orsini discloses the following:

c) a citizenship status and a current location of the access candidate and an existence of a data access agreement with a citizenship requirement, wherein the location requirement and the data access agreement requirement; (see Orsini paragraph [0013], lines 1-3; paragraph [0060], lines 4-13: management of secure data, parameters (i.e. attributes) agreement, location information)

d) the citizenship status and the current location of the access candidate with a citizenship requirement and a location requirement; (see Orsini paragraph [0013], lines 1-3; paragraph [0060], lines 4-13: management of secure data, parameters (i.e. attributes) agreement, location information)

It would have been obvious to one of ordinary skill in the art to modify Lee-Te for at least one of: an indication an existence of a data access agreement with the access candidate; a current location of the access candidate; and a citizenship status of the access candidate as taught by Orsini. One of ordinary skill in the art would have been motivated to employ the teachings of Orsini for a relatively fast, secure, and efficient authentication of data streams. (see Orsini paragraph [0012], lines 1-3; paragraph [0013], lines 1-3)

Regarding Claim 41, Lee discloses the method of claim 1.

Lee does not specifically disclose for supplemental evidence to verify the attributes. However, Orsini discloses receiving supplemental evidence verifying the attributes of

the access candidate. (see Orsini paragraph [0013], lines 1-3; paragraph [0060], lines 4-13: management of secure data, parameters (i.e. attributes) agreement, location information)

It would have been obvious to one of ordinary skill in the art to modify Lee for supplemental evidence such as current location to verify the attributes as taught by Orsini. One of ordinary skill in the art would have been motivated to employ the teachings of Orsini for a relatively fast, secure, and efficient authentication of data streams. (see Orsini paragraph [0012], lines 1-3; paragraph [0013], lines 1-3)

Regarding Claim 42, Lee discloses the system of claim 15, wherein the data subsets are separated into the at least one data class based on a data provider of the data. (see Lee col 6, lines 14-23: software functionality (authentication system: access device, terminal) implemented using C++; (implies object oriented programming language utilizing class data structures)

Regarding Claim 43, Lee discloses the method of claim 15, wherein the physical access comprises physical access to a facility housing the computer workstation. (see Lee col 6, lines 32-39: number of terminals provided to work with a number of access devices (implies facility to house terminal(s) separately or together); col 5, lines 40-44: terminal application software includes functionality to control terminal actions (such as logon actions))

Regarding Claim 44, Lee discloses the method of claim 15, wherein the physical access comprises logging on to the computer workstation. (see Lee col 6, lines 32-39: number of terminals provided to work with a number of access devices; col 5, lines 40-44: terminal application software includes functionality to control terminal actions (such as logon actions))

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carlton V. Johnson whose telephone number is 571-270-1032. The examiner can normally be reached on Monday thru Friday , 8:00 - 5:00PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a

USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Carlton V. Johnson
Examiner
Art Unit 2436

CVJ
September 12, 2011

/Nasser Moazzami/

Supervisory Patent Examiner, Art Unit 2436